UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/701,154	11/03/2003	Massimiliano Antonio Poletto	RIV-0510	5561

87555 7590 05/09/2012

Riverbed Technology Inc. - PVF
c/o PARK, VAUGHAN, FLEMING & DOWLER LLP
2820 Fifth Street
Davis, CA 95618

EXAMINER	
MEHRMANESH, ELMIRA	
ART UNIT	**PAPER NUMBER**
2113	
MAIL DATE	**DELIVERY MODE**
05/09/2012	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE BOARD OF PATENT APPEALS
AND INTERFERENCES

Ex parte MASSIMILIANO ANTONIO POLETTO, EDWARD W. KOHLER, JR., ANDREW RATIN, and ANDREW GORELIK

Appeal 2010-000814
Application 10/701,154
Technology Center 2100

Before MAHSHID D. SAADAT, DAVID M. KOHUT, and MICHAEL R. ZECHER, *Administrative Patent Judges*.

ZECHER, *Administrative Patent Judge*.

DECISION ON APPEAL

I. STATEMENT OF THE CASE

Appellants appeal under 35 U.S.C. § 134(a) from the Examiner's Final Rejection of claims 1-3, 5, 7-16, 18-22, and 28-32. Claims 4, 6, and 17 have been cancelled. Claims 23-27 and 33-36 have been allowed. Supp. Br. 2. We have jurisdiction under 35 U.S.C. § 6(b).

We affirm.

Appellants' Invention

Appellants invented a system, method, and storage medium for detecting network intrusions and other conditions in a network. According to Appellants, the claimed invention includes a plurality of collector devices that collect data and statistical information on packets that are sent between nodes on a network, and an aggregator device that receives such information from the plurality of collectors and produces a connection table that maps each node on the network to a record that stores information about traffic to and from the node. Moreover, the aggregator device runs multiple processes that determine network events by aggregating anomalies into network events. *See* Abstract.

Illustrative Claim

> 1. A system, comprising:
>
> a plurality of collector devices that are disposed to collect connection information to identify host connection pairs from packets that are sent between nodes on a network; and
>
> an aggregator device that receives the connection information from the plurality of collector devices, and which produces a connection table that maps each node on the network to a record that stores information about packet traffic to the node and traffic from the node, with the aggregator device further comprising:
>
> a process executed on the aggregator device to detect anomalies in connection patterns; and

> a process executed on the aggregator device to aggregate detected anomalies into the network events with the anomalies that are detected including denial of service attack anomalies and scanning attack anomalies.

Prior Art Relied Upon

Ontiveros	US 2002/0107953 A1	Aug. 8, 2002

Rejection on Appeal

Claims 1-3, 5, 7-16, 18-22, and 28-32 stand rejected under 35 U.S.C. § 102(e) as being anticipated by Ontiveros. Ans. 3-9.

Examiner's Findings and Conclusions

The Examiner finds that Ontiveros' table that stores information about network packet traffic between a source and a destination describes "a connection table that maps each node on the network to a record that stores information about packet traffic to and from the node," as recited in independent claim 1. Ans. 3 and 9. Further, the Examiner finds that Ontiveros' disclosure of monitoring source and destination addresses (*i.e.*, node to node connections) and identifying certain attack patterns describes a process executed on the aggregator device to detect anomalies in connection patterns, as claimed. Ans. 9-10. The Examiner also finds that Ontiveros' disclosure of detecting and denying data traffic with patterns that are in contrast to normal traffic patterns amounts to detecting events associated with network attacks. Ans. 3-4 and 10. Consequently, the Examiner finds that Ontiveros describes a process executed on the aggregator device to aggregate detected anomalies into the network events, as claimed. *Id.*

Appellants' Contentions

Appellants contend that Ontiveros' hit-count table only keeps a count of the number of times a source address is detected and, therefore, does not describe "a connection table that maps each node on the network to a record that stores information about packet traffic to and from the node," as recited in independent claim 1. Br. 10. Further, Appellants argue that Ontiveros fails to describe a process to detect anomalies in connection patterns and a process to aggregate detected anomalies into network events, as claimed. Br. 10. Appellants allege that Ontiveros only deals with detection of traffic patterns, whereas the claimed invention is directed to the feature of "connection patterns." Br. 11. Moreover, Appellants contend that while Ontiveros discloses thwarting attacks, Ontiveros does not describe a process that detects anomalies in connection patterns and determines whether the anomalies should be aggregated into events that can be associated with these types of attacks. Br. 12.

II. ISSUE

Did the Examiner err in finding that Ontiveros describes the following claim limitations recited in independent claim 1:

(a) "a connection table that maps each node on the network to a record that stores information about packet traffic to the node and traffic from the node[;]"

(b) "a process executed on the aggregator device to detect anomalies in connection patterns;" and

(c) "a process executed on the aggregator device to aggregate detected anomalies into the network events with the anomalies that are

detected including denial of service attack anomalies and scanning attack anomalies."

III. ANALYSIS

Claim 1[1]

We do not find error in the Examiner's anticipation rejection of independent claim 1. Independent claim 1 recites, *inter alia*:

> [1)] a connection table that maps each node on the network to a record that stores information about packet traffic to the node and traffic from the node[;] [2)] a process executed on the aggregator device to detect anomalies in connection patterns; and [3)] a process executed on the aggregator device to aggregate detected anomalies into the network events with the anomalies that are detected including denial of service attack anomalies and scanning attack anomalies.

At the outset, we adopt the Examiner's findings of fact as our own. In particular, we find that Ontiveros' hit-count table, which stores memory entries for each packet source using a hash table keyed by source and destination addresses (¶¶ [0038] and [0040]), amounts to a table containing records that store or catalog information about packet traffic to and from a network port or node. Consequently, we agree with the Examiner that Ontiveros describes "a connection table that maps each node on the network to a record that stores information about packet traffic to the node and traffic from the node," as recited in independent claim 1. *See* Ans. 3 and 9.

---

[1] If prosecution of the present patent application resumes, the Examiner should consider whether independent claim 1 is a hybrid claim having both system and method elements and, therefore, is indefinite under § 112, second paragraph. *See Rembrandt Data Techs., LP v. AOL, LLC*, 641 F.3d 1331, 1339 (Fed. Cir. 2011).

Alternatively, Appellants cannot rely solely upon the content or type of information stored in the claimed "connection table" to patentably distinguish independent claim 1 over the prior art of record. The content or type of such information is non-functional descriptive material, which is not entitled to any patentable weight. *See In re Lowry*, 32 F.3d 1579, 1583 (Fed. Cir. 1994) ("Lowry does not claim merely the information content of a memory [. . .] nor does he seek to patent the content of information resident in a database."). *See also Ex parte Nehls*, 88 USPQ2d 1883, 1887-90 (BPAI 2008) (precedential); *Ex parte Curry,* 84 USPQ2d 1272, 1274-75 (BPAI 2005) (informative), *aff'd*, slip op. 06-1003 (Fed. Cir. June 2006) (Rule 36).

Further, we find that Ontiveros' process of sorting data type attacks to identify new patterns (¶ [0050]) amounts to detecting abnormal packet traffic patterns between connected network ports or nodes. As such, we agree with the Examiner that Ontiveros describes "a process executed on the aggregator device to detect anomalies in connection patterns[,]" as recited in independent claim 1. *See* Ans. 10. Moreover, we find that Ontiveros discloses preventing hacking attacks on the network, including denial of service attacks and other attacks (*e.g.*, scanning attacks) (¶ [0003]), by detecting and denying packet traffic with abnormal traffic patterns (¶ [0024]). In particular, by detecting and denying packet traffic associated with denial of service attacks and scanning attacks, Ontiveros necessarily describes aggregating detected abnormalities into events associated with these types of attacks. Consequently, we agree with the Examiner that Ontiveros describes "a process executed on the aggregator device to aggregate detected anomalies into the network events with the anomalies that are detected including denial of service attack anomalies and scanning

attack anomalies[,]" as recited in independent claim 1. *See* Ans. 4 and 10. It follows that the Examiner has not erred in finding that Ontiveros anticipates independent claim 1.

Claims 5, 7, and 28

Appellants do not provide separate and distinct arguments for patentability with respect to independent claim 28, and dependent claims 5 and 7. *See* Br. 7-12. Therefore, since Appellants group independent claim 28, and dependent claims 5 and 7, with independent claim 1 (Br. 7), these claims fall with independent claim 1. *See* 37 C.F.R. § 41.37(c)(l)(vii).

Claims 2, 3, 8-13, and 29-32

Appellants reiterate what dependent claims 2, 3, 8-13, and 29-32 recite and generally allege that Ontiveros does not describe the additional claim limitations. *See* Br. 12-15. Merely pointing out what each dependent claim recites and nakedly asserting that the textual portions of Ontiveros relied upon by the Examiner does not describe the corresponding claim limitations does not amount to a separate patentability argument. *See* 37 C.F.R. § 41.37(c)(vii) ("A statement which merely points out what a claim recites will not be considered an argument for separate patentability of the claim."); *see also In re Lovin*, 652 F.3d 1349, 1357 (Fed. Cir. 2011) ("[W]e hold that the Board reasonably interpreted Rule 41.37 to require more substantive arguments in an appeal brief than a mere recitation of the claim elements and a naked assertion that the corresponding elements were not found in the prior art."); *cf. In re Baxter Travenol Labs.*, 952 F.2d 388, 391 (Fed. Cir. 1991) ("It is not the function of this court to examine the claims in greater detail than argued by an appellant, looking for [patentable]

distinctions over the prior art."). It follows that the Examiner has not erred in finding that Ontiveros anticipates dependent claims 2, 3, 8-13, and 29-32.

Claim 14-16

Appellants reiterate the same arguments set forth in response to the anticipation rejection of independent claim 1 to rebut the anticipation rejection of independent claim 14, and dependent claims 15 and 16. *See* Br. 14. We have already addressed these arguments in our discussion of independent claim 1, and we found them unpersuasive. It follows that the Examiner did not err in finding that Ontiveros anticipates independent claim 14, and dependent claims 15 and 16.

Claims 18-22

Appellants do not provide separate and distinct arguments for patentability with respect to dependent claims 18-22. *See* Br. 14-15. Therefore, since Appellants group dependent claims 18-22 with independent claim 14, and dependent claims 8-13 (Br. 15), these claims fall with independent claim 14, and dependent claims 8-13. *See* 37 C.F.R. § 41.37(c)(l)(vii).

IV. CONCLUSION

The Examiner has not erred in rejecting claims 1-3, 5, 7-16, 18-22, and 28-32 as being anticipated under 35 U.S.C. § 102(e).

V. DECISION

We affirm the Examiner's decision to reject claims 1-3, 5, 7-16, 18-22, and 28-32.

No time period for taking any subsequent action in connection with this appeal may be extended under 37 C.F.R. § 1.136(a)(1)(iv).

AFFIRMED

ELD